

CLAIMS

Sub
a3

1. Conditional access system decoder (9) comprising:
 - 5 - at least one device (12) intended to read and/or to write data from/to a detachable security element (10) supplied by a service provider;
 - filters (11) intended to select at least one message (EMM) for managing entitlements which a user 10 possesses with regard to a service supplied by the said provider from among a data stream (TS) received;
 - an access control module (CA) capable of:
 - a) receiving an identification parameter (AD) contained in a security element (10) inserted into the 15 said decoder;
 - b) installing a filter configuration (C1, C2) as a function of the identification parameter (AD) received in such a way as to select an entitlement management message (EMM) intended for the said inserted security 20 element (10); and
 - c) transmitting the said message (EMM) to the said inserted security element;
- characterized in that it furthermore comprises:
 - a module for storing entitlements (MD) capable of:
 - 25 i) storing said configuration of filters (C1, C2) which is installed by the access control module (CA);
 - ii) reinstalling, following the erasure of the configuration of filters consequent upon the removal of the said security element, the stored configuration of 30 filters which is appropriate to the said security element, in such a way as to select an entitlement management message (EMM) intended for the said security element when the latter is removed; and
 - iii) storing the said message (EMM) in a memory (14) of 35 the said decoder.
2. Decoder according to Claim 1, in which the module for storing entitlements (MD) is furthermore capable of:

iv) detecting the insertion of a security element into said decoder;

v) verifying whether an entitlement management message (EMM) intended for said inserted security element is stored in the memory (14) of the decoder; and

vi) should verification be positive, transmitting said stored message (EMM) to said inserted security element.

3. Decoder according to Claim 2, in which the module for storing entitlements (MD) detects the insertion of a security element (10) into the decoder by recording any new installing of configuration of filters by the access control module (CA).

4. Decoder according to one of Claims 1 to 3, in which the detachable security element (10) is a smart card.

5. Decoder according to Claim 4, in which the identification parameter (AD) contained in the security element is the address of the smart card.

20 6. Method of processing a message (EMM) for managing entitlements which a user possesses with regard to a service, said method comprising the steps consisting in:

- inserting a detachable security element (10) into a decoder (9);
- recovering (A3, A4) from said security element an identification parameter (AD);
- installing (A5) a configuration of filter of the decoder as a function of said identification parameter (AD) in such a way as to select an entitlement management message (EMM) intended for said inserted security element;
- transmitting (A6-A10) said message (EMM) to said inserted security element,

35 characterized in that the step of installing the configuration of filter which is appropriate to said security element is followed by a step of storing (B1, Bla) said configuration and in that, when said security element (10) is removed from the decoder, causing the

erasure (C2) of said configuration of filters, the configuration of filters which is appropriate to the removed security element is reinstalled (D2) on the basis of the configuration stored during the storage 5 step in such a way as to select an entitlement management message (EMM) intended for said removed security element.

7. Method according to Claim 4, characterized in that it comprises an additional step (D3, D3a) 10 consisting in storing in a memory (14) of the decoder said entitlement management message (EMM) intended for said removed security element when such a message is selected.

8. Method according to Claim 5, characterized in 15 that it furthermore comprises the steps consisting in:

- reinserting said security element (10) into the decoder;
- verifying whether an entitlement management message (EMM) intended for said inserted security 20 element is stored in the memory (14) of the decoder; and
- should verification be positive, transferring said stored message (EMM) to said inserted security element.

*ad&
a4* →